

CLAIMS

1. (Amended) An information recording medium in which a recording
mark is formed as main information by switching a signal level at a
5 predetermined interval of a reference signal,
wherein sub-information is recorded so as to be superimposed on the
main information by deformation of a shape or a pattern of the recording mark or
positional displacement of the recording mark in accordance with the
sub-information, the sub-information being subjected to data conversion based on
10 medium inherent information or apparatus nullification information that is
recorded on the information recording medium.
2. (Amended) The information recording medium according to claim 1,
wherein the medium inherent information is recorded irreversibly so
15 that only reproduction can be performed with respect to the medium inherent
information.
3. (Amended) The information recording medium according to claim 2,
wherein the medium inherent information is recorded in a burst cutting
20 area (BCA).
4. (Amended) The information recording medium according to claim 1,
wherein the data conversion of the sub-information is a correlation
operation of the sub-information with respect to a pseudo random number
25 sequence that is generated using the medium inherent information or the
apparatus nullification information as an initial value.
5. (Amended) The information recording medium according to claim 1,
wherein the data conversion of the sub-information is a correlation
30 operation of the sub-information with respect to a pseudo random number
sequence that is generated using as an initial value a contents encryption key
obtained using the medium inherent information or the apparatus nullification
information.
- 35 6. (Amended) The information recording medium according to claim 5,
wherein the apparatus nullification information is an encryption key set
for encrypting the main information of the information recording medium.

7. (Amended) An information recording apparatus, comprising:
a main information recording unit that records, in synchronization with
a predetermined reference signal, main information by forming a recording mark
at discrete reference positions on an information recording medium;

a random number sequence generating unit that generates a pseudo
random number sequence using as an initial value medium inherent information
or apparatus nullification information that is recorded on the information
recording medium; and

a sub-information recording unit that records sub-information so that
the sub-information is superimposed on the main information by deformation of a
shape or a pattern of the recording mark or positional displacement of the
recording mark, based on the sub-information and the pseudo random number
sequence generated by the random number sequence generating unit.

8. (Amended) The information recording apparatus according to claim 7,
wherein the medium inherent information has been read out in advance
from a burst cutting area (BCA) in which the medium inherent information is
recorded irreversibly so that only reproduction can be performed with respect to
the medium inherent information.

9. (Amended) The information recording apparatus according to claim 7,
wherein the apparatus nullification information is an encryption key set
for encrypting the main information, and the initial value for the random number
sequence generating unit is at least one encryption key set.

10. (Amended) An information reproducing apparatus, comprising:
a main information reproducing unit that reproduces main information
from a recorded mark having a length that is an integral multiple of a discrete
reference interval on an information recording medium;

a clock extracting unit that extracts a clock that is synchronized with
the reference interval from a reproduced signal obtained when the recorded mark
is reproduced;

a random number sequence generating unit that reads out medium
inherent information or apparatus nullification information that is recorded on the
information recording medium and generates a pseudo random number sequence
using the medium inherent information or the apparatus nullification information

as an initial value; and

- 5 a sub-information reproducing unit that reproduces sub-information based on the reproduced signal reproduced by the main information reproducing unit, the clock extracted by the clock extracting unit, and the pseudo random number sequence generated by the random number sequence generating unit.

11. (Amended) The information reproducing apparatus according to claim 10,

- 10 wherein by the sub-information reproducing unit, the medium inherent information has been read out in advance from a burst cutting area (BCA) in which the medium inherent information is recorded irreversibly so that only reproduction can be performed with respect to the medium inherent information

12. (Amended) The information reproducing apparatus according to claim 15 10,

wherein the apparatus nullification information is an encryption key set for encrypting the main information, and the initial value for the random number sequence generating unit is at least one encryption key set.